SOUTH AFRICAN PROPOSED LEGISLATION ON PROTECTION OF PERSONAL INFORMATION

A BANK'S PERSPECTIVE

Candidate number: 8004
Supervisor: Dr. L.A. Bygrave
Deadline for submission: September/04/2007

Number of words: 16,469 (max. 18.000)

04.09.2007

Content

1 Introduction

Privacy International[1] made the following statement regarding South Africa's financial sector in its 2005 world survey:

> *"South Africa has a well-developed financial system and banking infrastructure. Despite the sophistication of the financial sector, the privacy of financial information is weakly regulated by a code of conduct for banks issued by the Banking Council."*

This extract highlights some of the problems South Africa are experiencing with its current status on privacy as viewed from an International perspective. In recent years the International society has stepped up its efforts in creating a global village wherein the individual could be assured of having his/her privacy protected. Various conventions and guidelines[2] have previously laid the foundation for privacy but it was not until the European Union's (EU) launch of its Directive on Data Protection in 1995 that we have seen a real coerced shift in the focus of such protection. Cross border data transfers from the EU became something of the past unless third countries (those countries outside the EU) could prove the existence of adequate data protection provisions. It seemed to a big extend that international trade would be hampered and some of its biggest trading partners, such as the US, suddenly felt the impact due to its lagging protection measures. In order to curtail such inadequacies, a Safe Harbor Agreement was entered into between the EU and US whereby cross border data flow would be allowed under certain prerequisites. This Agreement however, does not cover Financial Institutions.

[1] Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression. Available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65428 (17 August 2007).

[2] a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and
b) the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

Concomitantly, South Africa, having the EU as its biggest trading partner also felt the grunt and some SA organizations had to take its processing to within the borders of the EU.[3] By implication it was then assumed that South Africa lacked the adequacy criteria as laid down by the EU Directive on Data Protection.[4] The South African Law Reform Commission (hereinafter referred to as SALRC) instructed a project committee to work on a draft Bill on Protection of Personal Information (hereinafter referred to as POPIA).

Some of the reasons why, can best be explained as Prof Iain Currie[5] reflects in his summary of the proposed POPIA:

> *"South Africa has general privacy protection in the Bill of Rights [s 14]. The right is protected by a private law action to interdict current or anticipated privacy infringements or to recover damages for infringements that have already occurred. Though information privacy is encompassed in the constitutional protection of privacy, there is no specific legislative regulatory regime for this aspect of privacy. The Promotion of Access to Information Act [6]protects personal information from disclosure in response to a request made in terms of the Act, but has no application outside the context of such a request. It is this absence of legislation that the SALRC draft Bill intends to remedy."*

Although there is current legislation in place, none are specifically formulated to address data protection. For instance, The Electronic and Communication Transaction (ECT) Act of 2002[7] also addresses the collection of personal

[3] Nedbank (one of the big five banks in South Africa) has accordingly been forced, in the absence of such legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements. This has resulted in the effective cost to market of the bank's outsourcing service being driven up and could very well be the reason for preventing the bank from obtaining further business processing outsourcing deals within Europe on the basis of not being cost competitive enough. (Comments on SALRC draft proposal)

[4] Art 25(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Also refer to Art 29 Working Party's Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data. (Annex to the Annual Report 1998 (XV D/5047/98) of the working party established by Article 29 of Directive 95/46/EC.)

[5] The members of the Project Committee for this investigation are:

[6] Act No. 54 of 2002. View www.info.gov.za/gazette/**act**s/2002/a54-02.pdf (12 August 2007)

[7] Art 50(2) ECT Act.

information in its chapter 8 but subscription to such principles is voluntary. The Regulation of Interception of Communications (RIC) Act prohibits the interception of communications while one Act that has recently been enacted, The National Credit Act, makes specific provision for the regulation of personal information, although such regulation is restricted to the financial sector.

Should the POPIA be enacted, consequential amendments may be necessary in respect of the following acts: Banking Act 38 of 1942, Broadcasting Act 4 of 1999, Copyright Act 98 of 1978, Electoral Act 73 of 1998, Financial Advisory and Intermediary Services Act (FAIS) 37 of 2002, Financial Intelligence Centre Act (FICA) 38 of 2001, Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002, Short-term Insurance Act 53 of 1998, Long-term Insurance Act 52 of 1998 and Telecommunications Act 103 of 1996.[8]

This thesis will aim to address the proposed POPIA and the subsequent influence or impact it might have on the banking sector, by also taking into account some of the more recent developments as prescribed in Basel II and The National Credit Act, although not much time will be spent on this.

It will proceed in several chapters, chapter 2 addressing the proposed co-regulatory scheme. We will see how this might affect the current Code of Conduct as laid down by the Banking Council. The first half of this chapter will look at various models of co-regulatory schemes and the success achieved in the implementation of such schemes, while the second category will propose a draft code. Chapter 3 will examine the Trans Border Data Flow impact on the transfer of Bank Customer data outside the borders of South Africa and also the extent to which the inclusion of juristic persons would affect such transfer. Chapter 4 will evaluate how Basel II processing will influence banks' current practice in terms of the POPIA.

Lastly, in chapter 5 I will conclude by ascertaining whether there is a golden solution to some of the problems that were discussed in the previous chapters.

[8] SALRC Discussion papers available at http://www.doj.gov.za/salrc/dpapers.htm (07 August 2007)

In doing so, it has to be emphasised that the proposed POPIA in its current version is still subject to change and where reference is made to specific sections, amendments might for future purposes render them obsolete. It is therefore my aim in addressing the various parts of this thesis based on the current version of the proposed POPIA, as is.

2 The current Banking Code of Practice and the proposed POPIA

Codes offer flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors. With or without legislation, codes will continue to be significant instruments by which organisational responsibilities are defined, employee obligations are communicated and citizen rights are established.[9]

If the proposed POPIA is to follow a co-regulatory scheme as is proposed by the SALRC, then the question has to be asked whether the current banking code of practice will suffice. It also has to be taken into account whether the code is indeed fulfilling the requirements of the National Credit Act.

The National Credit Act is consumer-protection legislation, aiming to regulate the market in consumer credit principally by improving access to credit and preventing unfair business practices.[10] The provisions relating to data protection are found in Chapter 4, part B thereof. Section 68 of the Act creates a right to confidential treatment of 'confidential information' received, compiled, retained or reported in terms of the Act. Confidential information is defined in s 1 as 'personal information that belongs to a person and is not generally available to or known by others'. The confidentiality of such information must be protected by its holder and must be used only for a lawful purpose, must be disclosed only to the person to whom it relates or to a third party where required by law, by court order or order of the Consumer Affairs Tribunal created by the Act or 'as directed by . . . the instructions of the consumer'. [11]

[9] Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at http://web.uvic.ca/polisci/bennett/

[10] Currie, I "The Data Provisions of the National Credit Act" available at http://wwwserver.law.wits.ac.za/mi/privacy/nationalcreditact.htm (05 August 2007)

[11] Id.

The Banking Association of South Africa revealed in March 2007 a code of conduct[12] specifically aimed at the selling of unsecured credit. In its paragraph 2.9 it states that it will comply with all relevant legislation and agreed Codes of Practice. It does however not make any specific mention of section 68 as contained in the National Credit Act.[13] Since our main focus will revolve round the Banking Code of Practice, I will not pay any further attention to the said code of conduct.

However, before it can be ascertain whether the Banking code of Practice will suffice, a synoptic review of the proposed POPIA will have to be done.

In the SALRC's discussion paper 109 on Privacy and Data Protection[14] it states that the preliminary recommendations of the SALRC, as set out in the Bill can be summarised as follow:

> a) Privacy and information protection should be regulated by a general information protection statute, with or without sector specific statutes, which *will be supplemented by codes of conduct*[15] for the various sectors and will be applicable to both the public and private sector. Automatic and manual processing will be covered and identifiable natural and juristic persons will be protected **[Chapter 2, clauses 3-6].**
>
> b) General principles of information protection should be developed and incorporated in the legislation. The proposed Bill gives effect to *eight core information protection principles, namely processing*

[12] See: http://www.banking.org.za/documents/2007/MARCH/InfoDoc_34753.pdf (03August 2007)

[13] **68.** (1) Any person who, in terms of this Act, receives, compiles, retains or reports any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information, and in particular, must-
(a) use that information only for a purpose permitted or required in terms of this Act, other national legislation or applicable provincial legislation; and
(b) report or release that information only to the consumer or prospective consumer, or to another person-
(i) to the extent permitted or required by this Act, other national legislation or applicable provincial legislation; or
(ii) as directed by-
(aa) the instructions of the consumer or prospective consumer; or
(bb) an order of a court or the Tribunal.
(2) Failure by a credit bureau to comply with a notice issued in terms of section ***55,*** in relation to this section, is an offence.

[14] Project 124, October 2005, Privacy and Data Protection.

[15] Own emphasis added.

limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability.[16] Provision is made for exceptions to the information protection principles **[Chapter 3, Part A, clauses 7-23]**. Exemptions are furthermore possible for specific sectors in applicable circumstances **[Chapter 4, clauses 32-33]**. Special provision has furthermore been made for the protection of special (sensitive) personal information **[Chapter 3, Part B, clauses 24-31]**.

c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission **[Chapter 5, Part A, clauses 34-46]**. The Commission will be responsible for the implementation of both the Protection of Personal Information Act (see Annexure B) and the Promotion of Access to Information Act, 2000. Data subjects will be under an obligation to notify the Commission of any processing of personal information before they undertake such processing **[Chapter 6, Part A, clauses 47-51]** and provision has also been made for prior investigations to be conducted where the information being collected warrants a stricter regime **[Chapter 6, Part B, clauses 52-53]**.

d) Enforcement of the Bill will be through the Commission using as a first step a system of notices where conciliation or mediation has not been successful. Failure to comply with the notices will be a criminal offence. The Commission may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence **[Chapter 8, clauses 63-87 and Chapter 9, clauses 88-92]**.

[16] Id.

e) *A flexible approach should be followed in which industries will develop their own codes of conduct (in accordance with the principles set out in the legislation) which will be overseen by the regulatory agency. Codes of conduct for individual sectors may be drawn up for specific sectors on the initiative of the specific sector or of the Commission itself.*[17] This will include the possibility of making provision for an adjudicator to be responsible for the supervision of information protection activities in the sector. The Commission will, however, retain oversight authority. Although the codes will accurately reflect the information protection principles as set out in the Act, it should furthermore assist in the practical application of the rules in a specific sector **[Chapter 7, clauses 54-62]**.

f) It is the Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Directive. In this regard a provision has been included that prohibits the transfer of personal information to countries that do not, themselves, ensure an adequate level of information protection **[Chapter 10, clause 94]**.

In both paragraphs a) and e) reference are made to codes of conduct. It is therefore unmistakably clear that South Africa will incorporate a co-regulatory scheme.

Currently, the Banking Code of Practice as provided for by the Banking Organisation of South Africa and to which all South African banks subscribe, is not legally binding. This flows from its introductory paragraph which states the following:

None of the provisions of this Code:

- *will be legally binding in any court of law;*

[17] Emphasis added.

- *may be used to influence the interpretation of the legal relationship between you and your bank;*
- *will give rise to a trade custom or tacit contract or otherwise between you and your bank.*[18]

In New Zealand, the approach is that codes of practice under its Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation.[19] Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. The proposed POPIA makes provision for codes in its section 62 to be legally binding.

In Australia an organisation or industry registering a Privacy Code under the Australian Privacy Act, must prove and be legally accountable for the Code providing at least the same level of protection that the ten National Privacy Principles of the Australian Privacy Act require – preferably more.[20]

The current South African code of practice in itself is not a Privacy Code and only makes provision in its paragraphs 4.5 – 4.7 for aspects related to the protection and processing of personal information.[21] It is also evident that the eight core information protection principles as proposed by the POPIA, namely processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability, are not all accounted for in the relevant paragraphs of the code.

In terms of Section 54(2) (a) of the proposed POPIA, a code of conduct must incorporate all the information protection principles[22] or set out obligations that,

[18] View at http://www.banking.org.za/consumer_information/consumer_information.htm (04 August 2007)

[19] See Part VI of the New Zealand Privacy Act.

[20] Comments on SALRC draft proposal by Michalsons.

[21] View at http://www.banking.org.za/consumer_information/consumer_information.htm (05 August 2007)

[22] A good example of a code of conduct that incorporates all the information protection principles was the 1996 Canadian Bankers Association Privacy Model Code. See discussion at http://web.uvic.ca/~polisci/bennett/research/cba.htm. (06 August 2007)

overall, are the equivalent of all the obligations set out in those principles[23]. A new Banking Code of Privacy is suggested that solely reflects these principles wherefrom a customer could then draw clear distinction on how his/her information would be processed without having to review the proposed POPIA in itself. In Section 54 (2) (b) of the proposed POPIA it states that a code of conduct must prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which these bodies are operating. This in itself will create consumer trust and make the POPIA more practically accessible by members of the public, ensuring its enforcement through knowledge. I dare say this based on the fact that members of the public are much more prepared in accessing codes located on a website, explained in laymen terms, than making a concerted effort in trying to analyse an Act.

The proposed POPIA states in its Section 54 (3) that a code of conduct may apply in relation to any one or more of the following –

(a) any specified information or class or classes of information;
(b) any specified body or class or classes of bodies;
(c) any specified activity or class or classes of activities;
(d) any specified industry, profession, or calling or class or classes of industries.

It is generally recognised that five kinds of privacy code can be identified according to their scope of application: organisational code, the sector code, the functional code, the professional code and the technological code.[24] It is therefore suggested that the Banking Industry in South Africa, would fall under the sector code[25], since the defining feature thereof is that there is a broad consonance of

---

[23] A further example of a code of conduct that set out obligations that, overall, are the equivalent of all the obligations set out in those principles is the Netherlands Code of Conduct for the Processing of Personal Data by Financial Institutions.

[24] Project 124, October 2005, Privacy and Data Protection.

[25] As allowed for by Section 54(3)(d) of the proposed POPIA.

economic interest and function and a similarity in the kinds of personal information collected.

The approach envisaged by the proposed POPIA seems to be on par with the co-regulatory scheme of Australia where any business or profession may develop a Code of Practice. The code must then be submitted to the Privacy Commissioner for approval. If the Code is deemed to be acceptable then the Commissioner may issue it.[26]

Section 55 (1) of the proposed POPIA states that the Commission *may*[27] issue a code of conduct under section 54 of the said Act on the Commission's own initiative or on the application of any person. Caution should however be thrown to the fact that this process in Australia has gone extremely slow with a relatively few number of businesses feeling the need to develop a Code of Conduct, relying solely on the Privacy Principles as set out in the Act.[28] If the same phenomenon plays itself out in the South African process, and the Commission becomes reluctant in issuing codes, the full effect or intention of the Act might never materialise. All of this will be due to an absence of knowledge on behalf of the consumer, or due to the lack of sector specific interpretation of the Act. It is suggested that the banking sector takes a pro-active role in submitting its own code of conduct instead of waiting on the Commissioner to suggest application or issue a code of its own.

[26] See Part IIIA of the Australian Privacy Act 1988 as amended.

[27] Own emphasis added.

[28] See: http://privacy.gov.au/business/codes/index.html (05 August 2007)

3 Trans Border Data Flow impact on transfer of bank data

Having the EU as its biggest trading partner, South Africa had to find a way in ensuring that its own proposed POPIA would fulfil the adequacy requirement as laid down in the EC Directive on Data Protection. In achieving this aim, a provision has been included that prohibits the transfer of personal information to countries that do not, themselves, ensure an adequate level of information protection.[29] Although this in itself seems to be justified with regard to the EU, it might cause serious implications for those trading partners and countries outside South Africa that do not have adequate levels of protection. Such an argument was posed by the Credit Bureau Association of South Africa in its submission to the SALRC:

> *"The majority of African States, if not all, have no information privacy legislation in place and subjectively it is foreseen that with the problems of the continent being what they are, the introduction of such legislation will not be seen for some considerable time. South Africa is presently increasing its presence on the continent and many South Africa organisations have offices throughout Africa. In effect this will mean that South Africa would isolate itself from the rest of the continent in its attempt to blindly follow directives designed for economies far removed from Africa and South Africa."*

To accommodate these fears certain exemptions, parallel to that of the EC Directive, were made. The relevant provision as embodied in Section 94 of the POPIA reads as follow:

A responsible party in South Africa may transfer personal information about a data subject to someone (other than the responsible party or the data subject) who is in a foreign country only if –

[29] Refer paragraph f), p 8 above.

(a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of this Act; or

(b) the data subject consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;
(ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;
(iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

For the purposes of this article it is important to understand the impact these exceptions might have on the Banking Industry. I will proceed by identifying three possible banking problems. The first being the prevention of fraud, the second being the execution of payment orders and the third relating to the transfer of legal persons' data.

3.1 Prevention of Fraud

Legislation was introduced in South Africa in 2003, aimed at preventing money-launderers, criminals and terrorists from abusing the country's financial system. The purpose of this legislation in the form of the Financial Intelligence Centre Act

(FICA)[30] is to protect all legal investments and finances and identify and prosecute all those involved in money laundering activities.

> *"South Africa has set itself a higher standard than even the United States and the United Kingdom. The South African Fica standard demands that all existing clients have to be Fica'd, whereas in the US and UK, for instance, it is only high-risk clients who had to be verified.*
>
> *It is understood that South Africa chose this route because, as the only African member of the Financial Action Task Force (FATF) on money-laundering, it was keen to show it could meet a higher standard."*[31]

Murray Michell, director of the South African Financial Intelligence Centre said in the same article that there is nothing in the law that prevents sharing Fica information but it is an issue between industries of shared costs and systems.. This would then imply that any bank customer's information under current legislation might be shared amongst industries and authorities, regardless of where in the world.

This statement is underlined in FICA's section 3(2)(b) where it states that apart from the Financial Intelligence Centre's principle objectives, some of its other objectives is to exchange information with similar bodies in other countries regarding money laundering activities and similar offences.

This is in line with how payment card organizations and banks which adhere to card payment schemes aim at protecting their customers and prevent fraud on a worldwide basis. They exchange information on individuals, for example, information on:

---

[30] Act Nr 38 of 2001, view www.fic.gov.za/info/a38-01b.pdf (07 August 2007)

[31] Fica'd to death, Mail and Guardian Online, 31 July 2006, view http://www.mg.co.za/personalfinance/articlePage.aspx?articleid=279307&area=/personal_finance/pers_fin_banking/ (07 August 2007)

- merchants participating in card payment schemes who default or have committed fraud;
- persons convicted or suspect of fraud (identifying data, type of fraud).

Information such as contained in these examples is exchanged at a worldwide level since criminal organisations specialising in card-based fraud operate throughout the globe and move their centre of activities according to the circumstances.[32]

The question would then arise as to whether such exchanging of information to third countries (specifically in Africa) that don't provide adequate data protection measures, would be legal in terms of the exclusions as is envisaged in the POPIA.

It is my opinion that none of the above exceptions authorise the transfer by banks of data to these countries for the prevention of fraud. If provision was made for a paragraph in the exclusions that would have read similar to that of Article 26(d) of the EC Directive;

> *(d) the transfer is necessary or legally required on important public interest ground…*

then maybe one could have argued that a measure to combat fraud would indeed have been interpreted as necessary based upon an important public interest.

Since none of the other African countries contain any adequate measures, one would then, in the absence of such a paragraph, have to argue that in terms of Section 94(a) the receiving country might be subject to a *binding scheme*[33] or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of the proposed POPIA.

---

[32] Professor Jan M.A. Berkvens and Marc N. Schauss; *The Amended proposal for an EC Directive on Data Protection; Progress on the face of it, disillusion after scrutiny* ; Butterworth's Journal of International Banking and Financial Law, 1993, February.

[33] Own emphasis added.

On September 17, 2006 the leaders of the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development, the European Investment Bank Group, the Inter-American Development Bank Group, the International Monetary Fund, and the World Bank Group agreed on a framework for preventing and combating fraud and corruption in the activities and operations of their institutions. This built on the work of a joint Task Force that was established on February 18, 2006 by the leaders of these institutions.

The institutions recognized that corruption undermines sustainable economic growth and that it is a major obstacle to the reduction of poverty. The leaders have outlined the following joint actions to combat fraud and corruption:

- agreement in principle on standardized definitions of fraudulent and corrupt practices for investigating such practices in activities financed by the member institutions;
- agreement on common principles and ***guidelines***[34] for investigations;
- agreement to strengthen the exchange of information, ***as appropriate and with due attention to confidentiality***[35], in connection with investigations into fraudulent and corrupt practices;
- agreement on general integrity due diligence principles relating to private sector lending and investment decisions;
- agreement to explore further how compliance and enforcement actions taken by one institution can be supported by the others.

Further, the institutions have agreed on continuing to work together to assist their member countries in strengthening governance and combating corruption, in cooperation with civil society, the private sector, and other stakeholders and institutions such as the press and judiciary with the goal to enhance transparency and accountability. [36]

[34] Id.

[35] Id.

[36] See http://www.adb.org/Media/Articles/2006/10629-regional-anticorruption/joint-statement.pdf (09 August 2007)

This framework might path the way to *binding schemes* as is proposed under Section 94(a) of the proposed POPIA, since most countries in Africa are members of the African Development Bank Group. It might also clear up the road for exchanging information to other countries outside Africa that don't have adequate protection measures.

The analogy that I am drawing from is that in the absence of having any clarification on what is meant by *binding schemes*, one has to purport that the drafters, having largely based their research and draft legislation inter alia on the EC Directive on Data Protection[37], must have had *binding corporate rules* in mind.

The UK's Information Commissioner's legal analysis and recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbour, sketches a good review of what Binding Corporate Rules entail:[38]

> *"The concept of using Binding Corporate Rules (BCR) to create adequate safeguards for the purposes of Article 26(2) was devised by the Article 29 Working Party in its working document on binding corporate rules, adopted on 3 June 2003 ('WP74')[39]. Subsequently, to assist with compliance, the Article 29 Working Party developed a model checklist on the content of a BCR application to Data Protection Authorities ('model checklist')and a co-operation procedure to facilitate the authorisation process (the 'co-operation procedure').*

[37] "Besides the international instruments, two national data protection laws have been particularly influential in the drafting of the Commission's proposed Bill. These instruments are the Netherlands' Wet Bescherming Persoonsgegevens (2000) (conforming closely to the EU Directive) and the New Zealand Privacy Act (1993) (conforming closely to the OECD Guidelines)." About the draft protection of Information Bill, I Currie, see http://wwwserver.law.wits.ac.za/mi/privacy/briefing.htm (11 August 2007)

[38] View http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf (10 August 2007)

[39] Working Document (WP74) Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN WP 74 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf. (10 August 2007)

BCR are internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards for the rights and freedoms of data subjects for the purposes of paragraph 9 of Schedule 4 to the Act. They are designed to be a global solution for multinational companies by ensuring their intra-group transfers comply with the Eighth Principle and providing a simple mechanism for obtaining the necessary authorisations across the EU. BCR must be submitted for approval by the Commissioner in order to obtain an authorisation which provides that transfers from the UK may be made within the group on the basis of the BCR."[40]

In light of the above, it is my opinion that a binding scheme, derived from the abovementioned framework, read as BCR, could in fact attribute to possibly the only short term solution in combating fraud and other illegal activities, without contravening the proposed POPIA. In the absence thereof, banks might be reluctant to report fraud due to its fear of contravening the POPIA. An example of such reluctance is found in Europe where the payment card sector's national and cross-border fraud prevention databases rely on input from banks. As the EU Data Protection Directive is not applied in the same way in all national legislation, banks in certain Member States have been reluctant to report fraudulent merchants to these databases, as they were concerned about possible breaches of national data protection laws. In view of the ever increasing numbers of fraud, the EU Committee of Data Protection Authorities ("Article 29 Working Party") has endorsed guidelines on the collection and processing of data on merchants whose contracts to accept payment cards have been terminated. The guidelines will help banks prevent fraud and ensure that merchants' privacy is better protected. Databases on "terminated" merchants are very important for the banking industry. However, the transfer of data to non-EU countries is not covered by the guidelines. The card schemes will carry out these transfers in compliance with the

[40] Ibid note 38.

rules in the Data Protection Directive, including by using standard contractual clauses. The banks have asked the Commission to re-establish legal certainty.[41]

3.2 Execution of Payment Orders[42]

Within the framework of their service, financial institutions in South Africa exchange personal data with subsidiaries and other financial institutions established outside South Africa. This relates in particular to transactions relating to the settlement of orders from customers or potential customers. These orders may reach a financial institution in the form of regular orders, but also in the form of electronic orders or requests for information through the Internet. The processing of personal data relating to such orders falls within the scope of the processing definition as set out in the proposed POPIA.

Similarly, a payment order is an order directing transfer of funds to a designated account or beneficiary. Payment orders may be sent by mail (or private courier), telex message, or through the Society for Worldwide Interbank Financial Telecommunication (Swift), a communication network widely used in international banking. The execution of a payment order therefore may imply the intervention of several banks. One will have the originating bank, the beneficiary bank and sometimes, if necessary, intermediary banks. There might also possibly be a card payment organization.

All the necessary information related to the originator of the order and the beneficiary, will be processed by the banks. Such information processed identifies the originator and the beneficiary in the form of their account numbers, names and addresses and it will often also identify the reason for payment. To successfully process a payment order, all the banks involved must transmit both data for the purposes of identification and any messages which accompany the payment order. The originating bank and the beneficiary's bank must perform accounting

[41] See http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/246&format=HTML&aged=0&language=EN&guiLanguage=en (12 August 2007)

[42] Most of what is argued here in is derived from an article that was written in the February 1993 Butterworth's Journal of International Banking and Financial Law, titled; *The Amended proposal for an EC Directive on Data Protection; Progress on the face of it, disillusion after scrutiny* by Professor Jan M.A. Berkvens and Marc N. Schauss.

operations relating to the debiting of the originator's account and the crediting of the beneficiary's account respectively.

It could be queried whether the processing and subsequent transfer inherent in the execution of payment orders are adequately covered by any of the exceptions as referred to above in Section 94 of the proposed POPIA. It is also not clear from this section whether the data subjects referred to are South African citizens, South African residents or also residents of third countries. Since the execution of a payment order generally involves at least two data subjects (as seen above), if residents of third countries which do not ensure an adequate level of protection are to be protected, then the transfer which is envisaged must fall within one of the five categories of exceptions mentioned earlier with respect to *all* data subjects involved. These exceptions will be dealt with separately here. I will deal with the first exception mentioned under the POPIA, lastly.

3.2.1 Data subject consent to transfer

There were various interpretations of consent in the SALRC's discussion paper 109 chapter 4 which deals with the information principles.[43] I will highlight some of these.

It was for instance contended that consent for the processing of nonsensitive information will be regarded as valid if it amounts to a freely given, specific and informed indication of the wishes (volunté) of the data subject - but that this volunté can be expressed in a variety of ways and that (other than with regard to sensitive information, for which it needs to be express) it does not necessarily need to be put in writing. Thus, for instance, if a person was informed of an intention on the part of a responsible party to use his (non-sensitive) information for a specific purpose, and was offered an opportunity to object to this use (e.g., by means of a negative tick-box on a form), yet did not use this opportunity (i.e. by

[43] See http://www.doj.gov.za/salrc/dpapers/dp109_prj124/CH%204%20PRINCIPLES%20OF%20INFORMATION%20PROTECTION.pdf (13 August 2007)

returning the form without the box being ticked), his consent to the use of his information can be inferred from this (in) action.

In Issue Paper 24 the question was posed whether the opt-out approach would constitute valid consent. Responses were varied. It was argued that the "opt-out" approach implies implicit consent; and would constitute valid consent, provided it meets all the criteria of implied consent required by the common law and set out in the privacy instruments. The banking industry explained that it has adopted the opt-out approach[44] since there is no clear guidance in South African legislation as to how the 'consent' issue should be addressed and also because of the prohibitive costs and administration should consent have to be sought for each and every application of personal information.

It was argued that a clear distinction is necessary between the use of personal information for marketing of services and products, and the use for processing product applications, verification of personal details, credit assessment, fraud prevention and statutory reporting obligations (FICA for instance). In order to make the distinction clear, the Banking Council has, for instance, treated marketing of products and other uses of personal information separately in the new Code of Banking Practice.[45]

---

[44] In the new Code of Banking Practice, effective from June 2004, the consent issue is dealt with as follows:
"4.7.1 Information about your personal debts and/or the manner in which you conduct your accounts may, in appropriate circumstances, be disclosed to credit risk management services where:
- you have fallen behind with your payments or you are in default with the terms of a product or service, and you have not made satisfactory proposals to us for repayment of your debt following formal demand and you have been given at least 28 calendar days' notice of our intention to disclose; or
- you have given us written, electronic or in the case of telephone banking, verbal consent; or
- your cheque is referred to drawer, in which case the information may be placed on a cheque verification service.
4.7.2 In respect of the marketing of services or products if you are:
- a new client, we will obtain your consent at the beginning of your relationship with us;
- an existing client we will inform you that you may withhold or withdraw your consent and how to exercise that choice. If you do not withhold your consent, we will presume that you agree to us continuing to market the services or products With your consent we may:
- bring to your attention details of our services and products, which may be of interest to you;
- give certain information about you to other subsidiaries within our group for marketing purposes;
- inform you about another company's services or products and, if you respond positively, you may be contacted directly by that company.
We will not pressurise you by suggesting that access to any our services and products is conditional upon your consent".

[45] **Confidentiality and privacy**
We will treat all your information as private and confidential (even when you are no longer a client). Except as set out in 4.7.1 below, we will not disclose any information about your accounts or your personal details to anyone, including other companies in our group, other than in four exceptional cases permitted by law. These are:
- where we are legally compelled to do so;
- where it is in the public interest to disclose;
- where our interests require disclosure (This will not be used as a reason for disclosing information about you or your accounts [including your name and address] to anyone else including other companies in our group for marketing purposes);
- where disclosure is made at your request or with your written or verbal consent. If you make use of electronic banking facilities like telephone banking, and the telephone calls are recorded, consent to disclosure might be recorded verbally.

It was submitted that an opt-out approach represents a proportional balance between protecting a consumer's privacy and the reality of modern business marketing strategies. It was furthermore stated that this approach is similar to the approach suggested in Article 14 of the EU Directive in respect of the data subject's right to object.[46] A consumer should be able to opt out at any time subject to reasonable limits, e.g. giving the company reasonable time to make the opt out effective.[47]

It was, however, noted that the question about opt-in *versus* opt-out forms of consent is one that has become particularly pressing, given the USA's recent federal legislation about spam117(H.R.2515 Anti-Spam Act of 2003).[48]

One of the clearest arguments against allowing opt-out in this context has been written by David Harris. His argument is simple (and has been used by others as well) that by legitimising optout it becomes an acceptable option for business to send unsolicited marketing material as long as they allow recipients to opt-out. This can potentially require so much effort from the recipient, that the recipient can be effectively overwhelmed by the number of received e-mails.[4950]It was concluded

---

5.1 Provision of credit
5.1.1 We will market and approve credit responsibly (based on the information you supply to us), to match your borrowing requirements and capabilities and supply you with suitable products, in an attempt to ensure that you are not extended beyond your financial means. However, our ability to do so depend on your compliance with our expectations of you set out in 5.11.4 regarding your financial affairs.
5.1.2 All lending will be subject to an assessment of your ability to afford and willingness to repay. This assessment may include:
- taking into account your income and expenses, including the dependability of your income;
- how you handled your financial affairs in the past;
- information obtained from credit risk management services and related services, and other appropriate parties, for example, employers, other lenders and landlords;
- how you have conducted your previous and existing accounts with us;
- information supplied by you, including verification of your identity and the purpose of the borrowing;
- credit assessment techniques, for example, credit scoring;"

[46] A specific right to object is laid down in some data protection laws. The EU Directive contains important instances of such a right, namely in Art 14 (a) (right to object to data processing generally), Art 14(b) (right to object to direct marketing) and , most innovatively, Art 15 (1) (right to object to decisions based on fully automated assessments of one's personal character). These rights to object are not found in other main international data protection instruments; See Chapter 11 of the Bill dealing with the rights of the data subject.(See however, the ILO Code of Practice on Protection of Workers' Personal Data). Neither have they existed in the bulk of national laws though this situation no longer pertains in Europe due to the adoption of the Directive; Bygrave ***Data Protection*** at 66.

[47] Comments made by Sanlam Life; Legal Service.

[48] Comments by Prof Martin Olivier.

[49] Id.

[50] Another example referred to by Prof Olivier, is that it is currently possible to opt-out of cookie-collection by DoubleClick — one of the largest collectors of web-related consumer behaviour. However, most consumers will neither be able to establish how to opt-out, nor understand the technology involved to opt-out (and therefore find it hard to establish whether opting out is a safe proposition). Worse, one can just imagine the effort required to locate and opt-out of all such services. And it is hard to imagine what new services will be established in future; again expecting the consumer to keep abreast of such new services and opting out of each is unrealistic. I suggest that the possibility to opt-out is not a valid form of consent for any 'service' that directly affects the consumer, such as sending unsolicited bulk e-mail. The case where it potentially has an

that the way in which the consent provision is to be implemented will have to be set out in the codes of conduct of the different sectors as approved by the Information Commissioner, or in relevant regulations.

The question which remains is whether the definition of consent makes allowance for "implied consent" (tacit consent) in the banking sector.

Section 2 of the POPIA states that **"consent"** means any freely-given, *specific* and *informed* expression of will whereby data subjects agree to the processing of personal information relating to them.[51]

In reviewing the Oxford English Dictionary it is interesting to note that the adjective *"express"* is explained as *"stated clearly"* but also as *"specific"* which in itself is described as *"clearly defined or identified"* and *"precise and clear"*. *"Informed"* in the abovementioned dictionary can be interpreted as *"having or showing knowledge"*.

To bring it into context, for consent to be valid, it has to be specific (i.e. it should relate to a specific piece of data processing by a specific responsible party for clearly defined purposes) and informed[52] (i.e. that the data subject must have had certain information at his disposal, principally knowledge of the potential recipients of the data).

It is therefore my opinion, unlike some of the other opinions as discussed above, that a data subject's consent to transfer, as required by section 94 (b) of the POPIA, has to be express consent.

It is doubtful whether it can be deduced from the fact that the originator has issued a payment order to which he has given his express indication of his consent. Indeed, whilst the originator may be viewed as having acquiesced to his bank

---

indirect effect on consumers — such as when tracking cookies are placed on a user's disk — is more problematic and needs serious discussion to attempt to identify.

[51] I draw conclusion from this that this definition will also be relevant to the transfer of information on data subjects.

[52] Section 2 of the POPIA **"consent"** means any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal information relating to them.

performing the processing and subsequent transfer implicit in giving the payment order, his consent is however tacit. Beyond transfer, the same is true with regards to the processing performed by any other banks involved. It also applies to the processing of data relating to the beneficiary and any third parties mentioned on the payment order.

It is therefore unlikely that a payment order can be issued without obtaining the express consent of the data subject which is as illustrated above, not common practice in the issuing of payment orders. It is also unlikely whether the consent of the beneficiary (which is also classified as a data subject) could have been acquired.

3.2.2 The transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request

This exception can be read in two parts, that which relates to the performance of a contract and the second part of the exception which makes provision for transfers made in the framework of pre-contractual measures. This second part does not apply since payment orders are generally not executed within such a framework. I will therefore focus on the first part.

What is strikingly remarkable about this and other exceptions is the fact that the drafters have opted to make use of the words individual and organisation, words to which no definitions are ascribed to in the proposed POPIA. In the absence thereof, it seems to be the logical approach that they should be open for interpretation, and if compared with Article 26 (1) of the EC Directive on Data Protection, for the purposes of this article be read as data subject and responsible party[53], respectively. However, it might also be argued that the drafters had specifically refrained from using these words in order to allow for either the individual or the organisation to fulfil the role of the responsible party and maybe even that of processor. I will illustrate this point at the hand of the EC Directive on Data Protection.

[53] This has a similar meaning than data controller in the EC Directive.

Art 26(1)(b) of the EC Directive reads as follow: *The transfer is necessary for the performance of a contract between the data subject and the controller….*

This article is ambiguous in its wording. An important question is whether a transfer by an intermediary bank might be authorised on the basis of the contract between the originator of the payment order and his bank. The wording refers to a contract between *the data subject* and *the controller* rather than to a contract between *a data subject* and *a controller*. This would make it clear that transfers necessary to perform a contract between the data subject and a controller are authorised even when executed by a controller who is not party to a contract with the data subject. In case the payment is then routed through an intermediary bank, it is the latter (also a controller) which makes the transfer to the third country, but in fact has no contractual relationship with the data subject. In the absence of this however, unless the customer is deemed to be the controller and his bank the processor; it would appear that an intermediary bank would be unable to transfer personal data to a third country which does not ensure an adequate level of protection. One might argue that this problem is resolved by Art 26(1)(c) (similar to that of section 94(d) of the proposed POPIA) where provision is made for a contract concluded in the interest of the data subject between the controller and a third party. What makes this problematic, is the fact that the definitions allocated to controller and processor do not resolve the question of whether it is the customer or his bank (and subsequent banks in the chain) who would be deemed to be the controller in the transfer of funds. It must be asked therefore whether the bank in this case, would not be acting as a processor on behalf of the customer. This problem is seemingly overcome by the SALRC drafters improvising the use of the words individual and organisation, allowing these words to be interpreted as a data subject, processor or responsible party (controller under EC Directive). But, if this is to be argued, then it seems illogic for the drafters to have started the section by making use of the words responsible party and data subject instead of organisation and individual. It reads as follow:

A responsible party in South Africa may transfer personal information about a data subject to someone (other than the responsible party or the data subject) who is in

a foreign country….if…(followed by the exceptions). To further illustrate the problem, here again, as mentioned earlier, since the execution of a payment order generally involves at least two data subjects (as seen above), if residents of third countries which do not ensure an adequate level of protection are to be protected, then the transfer which is envisaged must fall within one of the five categories of exceptions mentioned earlier with respect to *all* data subjects involved. This makes the interpretation of *a* data subject and *the* data subject difficult to follow and unclear to which data subject is referred.

The use of individual and organisation is in my opinion ambiguous and causes doubt to whether individual could also further be read as a juristic person, or whether the juristic person is in fact the organisation. I will further discuss this below under Juristic Persons.[54]

I find therefore that this exception is not sufficient to cover payment orders due to the ambiguity of its contents.

3.2.3 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party

This exception seemingly provide a solution for the use of intermediary banks during payment orders in the sense that it is not necessary for the individual to have a separate contract with the intermediary bank (and subsequent banks in the chain) as described above. On the basis of the wording it seems perfectly normal and acceptable. However, in my opinion, it is not clear what is meant by "…concluded in the *interest* of the individual..."

To sketch a scenario; if an individual's personal information is transferred to the United States, a country that does not provide adequate data protection measures, and the individual's personal information is then subjected to scrutiny, as for example through a summons that is issued under the US Patriot Act of 2001 by its subsequent authorities, is such a contract concluded then to be interpreted as "in

[54] See paragraph 3.3 below.

the interest" of the individual? I doubt it and can therefore not foresee that such an exception would suffice. This brings us to the next exception.

3.2.4 All of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;

(iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

Here as with the previous exception, it is hard to see how a payment order, would be validated under this exception. "Interest" is described in the Oxford English Dictionary as a "person's advantage or benefit", bringing benefit then within the context of interest, resulting in the same conclusion as argued above under par 3.2.3. If one argued that the contract was concluded in the financial or economic interest or benefit of the individual, then it might indeed suffice, but this was clearly not the intention of the drafters since it would limit the scope and application of the act to a specific sector. It is stipulated by the POPIA that all three the above scenarios have to be present. Without the fulfilment of the first scenario, I find it unnecessary analyzing the remaining two paragraphs of the exception. This brings as to the first exception, which is dealt with last.

3.2.5 The recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of this Act

This exception seems to be the only viable and unambiguous option for the execution of a payment order that has a beneficiary outside the borders of South Africa. It is still unclear on who the task will rest to make the decision as to whether a law, binding scheme or contract does indeed effectively uphold the principles and on what criteria such a decision must rest. It is advisable that a working party as suggested in section 45 of the proposed POPIA does a preparation of a methodology for evaluating the adequacy, in similar fashion as

was done in 1998 by the Working Party established by Article 29 of the EU Directive on Data Protection. With regards to contracts, it is suggested that a section 45 working party, provides guidelines to such contractual clauses as is reflected in the Commission Staff Working Document on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries.[55]With regards to binding schemes, I suggest, if they could be interpreted as Binding Corporate Rules as I successfully or unsuccessfully tried to illustrate earlier[56], a section 45 working party should follow the lead of the Article 29 Working Party in its working document on binding corporate rules, adopted on 3 June 2003 ('WP74').[57]If this could be done, without too many delays after enactment, it would most definitely provide clear guidelines for the various industries and sectors. This brings me to the issue surrounding the inclusion of juristic persons within the ambit of the proposed POPIA.

3.3 Juristic Persons

In the Issue Paper of the SALRC, the following points were made:

- *"Firstly, that the South African courts apply the common law principles developed for the protection of the privacy of natural persons also to juristic persons[58]: In* ***Financial Mail (Pt) Ltd v Sage Holdings Ltd***[59] *the court expressed the view that the actio iniuriarum should be available for a violation of the privacy of a juristic person even if one cannot, in the case of a juristic person, speak of feelings being outraged or offended. The basis for this protection is that privacy, like reputation (fama), can be infringed without injured feelings.*[60] *The court in* ***Janit v Motor Industry Fund***

[55] (2001/497/EC and 2002/16/EC).

[56] See par. 2.1 above.

[57] Working Document (WP74) Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN WP 74 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf. (14 August 2007)

[58] See **Motor Industry Fund Administrators (Pty) Ltd v Janit** supra at 60 (confirmed on appeal: 1995 4 SA 293 (A)) and **Financial Mail v Sage Holdings** supra 462-463***; Neethling's Law Of Personality*** 32 fn 336, 68ff, 71-73.

[59] Supra

[60] At 462; ***Neethling's Law of Personality*** at 71.

Administrators (Pty) Ltd[61] *affirmed the view expressed in the Sage Holdings case that a company would be entitled to regard the confidential oral or written communications of its directors and employees as sacrosanct and would, in appropriate circumstances be entitled to enforce the confidentiality of such communications. Interestingly, in the Janit case, the view was articulated that the theft of confidential discussions of a board of directors constituted an unlawful invasion of their privacy and any disclosure of such information, would itself constitute an invasion of the respondent's privacy.*[62]*Furthermore, where another person, who was aware that the information was unlawfully obtained and that they contained private and confidential discussions of the respondent's directors, helped himself to that information, such a person thereby violated and infringed their right to privacy.*[63]

- *In the second place the Constitution sets out the applicability of the Bill of Rights to a juristic person in s 8(4) of the Constitution which states: A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.*

- *Thirdly, in* ***Investigating Directorate: Serious Economic Offences ao v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao***[64] *it was held that juristic persons enjoy the right to privacy, but is not protected to the same extent as natural persons since juristic persons are not the bearers of human dignity. The level of justification for any particular limitation of the right would have to be judged in the light of the circumstances of each case.*

- *Finally, it was noted that it would appear that only natural persons (i.e. not juristic persons) are protected by the provisions of the* ***Promotion of***

[61] 1995 (4) SA 293 AD.

[62] At 303.

[63] At 305 B-D.

[64] Supra

***Access to Information Act**, since "personal information" is defined as information about an identifiable individual."*[656667]

In consideration of the above mentioned points, the SALRC proposed to include information pertaining to both natural and juristic persons in the ambit of the POPIA. The definition of "personal information" was therefore drafted to include a juristic person.[68] It can be deduced that the definition of "data subject", which means the *person* to whom personal information relate, includes a juristic person.

This in itself might pose a problem with regards to the ease of how corporate financial transactions would be dealt with across borders. Currently there are four European Member States that apply their data protection laws to legal persons,

[65] The definition of "personal information in PAIA reads as follows:
"Personal information" means information about an identifiable individual, including, but not limited to
a)information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
c) any identifying number, symbol or other particular assigned to the individual;
d) the address, fingerprints or blood type of the individual;
e) the personal opinions, views, or preferences of the individual, except where they are about another individual, or about a proposal for a grant, an award or a prize to be made to another individual;
f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the individual;
h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.

[66] Roos thesis at 499

[67] The definition of "personal information" in the **Electronic Communications and Transactions Act** is based on that of **PAIA**. It is furthermore interesting to observe that the Promotion of Access to Information Act 2 of 2000 (PAIA) lists amongst the grounds on which the refusal to grant access to the records of private persons is the mandatory protection of the privacy of a third party who is a natural person. No such exclusionary provision is made in respect of juristic persons.

[68] **"personal information"** means information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:
a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
c) any identifying number, symbol or other particular assigned to the person;
d) the address, fingerprints or blood type of the person;
e) the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the person;
h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
i) the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years;

namely Austria, Denmark, Italy and Luxembourg. The other European members only apply their data protection laws to natural persons. As this already poses a harmony problem for inter European data transfers, it is obvious to see the implications this might have for financial transactions between South Africa and those European states that don't offer protection laws to juristic or legal persons.
As already mentioned earlier, section 94 of the proposed POPIA states that a responsible party in South Africa may transfer personal information about a data subject to someone (other than the responsible party or the data subject) who is in a foreign country *only if* –

> *the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of this Act*;

It is my submission that in the absence of extending their protection to juristic persons, it would be doubtful whether it can be argued that recipients in such countries are subject to laws which effectively uphold principles for fair handling of the information. This would then imply that financial institutions or banks that transfer financial information related to its corporate customers would have to make provision for binding schemes or contracts for the majority of its European counterparts, rendering one of the initial purposes of section 94 obsolete.

Some of the arguments by the SALRC for the inclusion of section 94 were for instance that trade with African countries would be more difficult than with Europe since adequacy will have to be established in each particular transfer. It further argued that the legislation will improve the country's position regarding countries that do have proper legislation in place.[69]

Although South Africa would probably fulfil the adequacy requirement as envisaged by Article 25 of the EC Directive on Data Protection, most of its European counterparts won't fulfil the equivalent South African requirement,

[69] See http://www.doj.gov.za/salrc/dpapers/dp109_prj124/CH%207%20CROSS-BORDER%20INFORMATION%20TRANSFERS.pdf (15 August 2007) View page 14 thereof.

making trade from South Africa between itself and Europe, just as difficult as trade with African countries.

A good example with a two folded problem that might arise for banks would for instance be if a South African company transfers money to a European company. In doing so, most banks[70] make use of SWIFT. SWIFT is a worldwide financial messaging service which facilitates international money transfers. SWIFT stores all messages for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to as "mirroring". The messages contain personal data such as the names of the payer and payee. As a Belgian based cooperative, SWIFT is subject to Belgian data protection law implementing the EU Data Protection Directive.[71]

The first side of the problem can be viewed as follow; since Belgian law does not extend its data protection to juristic persons, the South African bank will have to make use of binding schemes or contracts. This would be its only alternative, unless express consent (which is impractical as explained under my paragraph 3.2.1) could be obtained from the data subject, since section 94 paragraphs c, d and e[72] of the proposed POPIA only refer to an individual. As mentioned above in my paragraph 3.2.2 I will illustrate this point here.

“Individual” is not defined in the proposed POPIA. The question would arise whether individual could refer to a juristic person. In South Africa, statutory interpretation in short is done by analysing the following methods;

- Purpose of the legislation;
    - Constitutional demands;

[70] See http://www.swift.com/index.cfm?item_id=41766 (15 August 2007)
[71] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) by Article 29 Working Party adopted 22 November 2006.

[72] (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
(e) all of the following apply:
(i) the transfer is for the benefit of the individual;
(ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;
(iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

- the primary rule of interpretation is to establish the purpose of legislation in the light of the Bill of Right;
- Meaning of the text;
- Balance of text and context;

- Other basic principles;
  - Legislation must be read as a whole;
  - The presumption that legislation does not contain futile or nugatory provisions. [73]

From the above it would seem futile and nugatory if the drafters had not indeed intended the interpretation of the word "individual" to include a juristic person, taking the purpose of the proposed POPIA and the balance of the text and context seen from a constitutional perspective. However, without even having to analyse all the methods of interpretation above, an answer can be deduced from the issue paper presented by the SALRC. In the issue paper, it was noted that it would appear that only natural persons (i.e. not juristic persons) are protected by the provisions of the Promotion of Access to Information Act, since "personal information" is defined as information about an identifiable "individual"[74]. This then clearly links the word "individual" up with a natural person, and not a juristic person.

The other side of the problem faced by banks is illustrated at the hand of the recent SWIFT investigation as explained by an opinion delivered by the Independent Centre for Privacy Protection at the federal state of Schleswig-Holstein (ICPP) on August 23rd, 2006:

> *"In international transfer of messages in relation to financial transfers between financial institutions the bank/ financial institution receiving an order by its customer is responsible for complying with privacy protection regulations and for the confidential use of personal data on its way to the financial institution receiving the transfer.*

[73] Christo Botha, Statutory Interpretation: An introduction for students (4th ed. Juta 2005).

[74] Own quotation.

The commissioned institutions as far as they have entrusted legally independent companies with data processing - especially forwarding of messages relating to financial transactions are responsible to ensure the level of data protection of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) in an unbroken chain by contract all the way to the data receiving financial institution.

Involving third parties that assist with the forwarding of client data for the purpose of routing, a specific international wire transfer is a case of data processing on a commissioned basis under section 11 of the German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG). The bank instructed to transfer money is responsible for providing an unbroken chain of written contracts with all financial institutions involved guaranting (sic) a constantly high level of protection as required by the provisions of the Federal Data Protection Act and the data concerned.

SWIFT acts as an agent or subcontractor of the data controller, the members of the SWIFT-group. At present, SWIFT does not provide for sufficient privacy protection guaranties that would justify transmitting personal data to be processed by SWIFT. Particularly lacking is a privacy protection measure comparable to the one provided in section 11 BDSG that would ensure SWIFT to be bound to instructions and confidential use of entrusted bank customers´ data.

SWIFT maintains a database in the United States of America which includes data records of European citizens that do not have contractual relations to U.S. agencies or U.S. banks. The transfer of this data by SWIFT/Europe to SWIFT/U.S.A. is illegal due to the lack of a sufficient legal basis. So far measures to ensure an adequate level of data protection for customer data being processed in the USA after articles 25 and 26 of the EC directive have not been taken at all."[75]

In a report issued on November 22, 2006, the Article 29 Working Party concluded that SWIFT, which provided the US Department of Treasury (UDT) with access to large amounts of financial data emanating from large financial institutions world

[75] View https://www.datenschutzzentrum.de/wirtschaft/swift/060825_swift_en.htm (15 August 2007)

wide, as well as the financial institutions were jointly liable for the violation of EU Data Protection Directive 95/46/EC by transferring personal data in a "confidential, non-transparent and systematic manner for years."

This then would imply that it would also be illegal in terms of the South African proposed POPIA to make use of SWIFT, since its operations would, as above explained under articles 25 and 26, also lack a sufficient level of adequacy as required by section 94 of the proposed POPIA.

To counter this problem in light of the case and its outcome, it is recommended that all companies and, in particular, banks, consider developing and implementing an action plan that will prepare them for future governmental demands for data. According to Jacqueline Klosek & Lauren Troxclair in their article titled: "Banks Need A Disclosure "Action Plan""[76], it is suggested that a three step plan should be implemented.
The first step mentioned is to plan ahead. Taking initiative by developing a proactive strategy is a responsive approach financial institutions can take to address some of the Working Party's conclusions. They further suggest that financial institutions should specifically negotiate for data protection and privacy law compliance provisions in contracts with financial fund transfer services such as SWIFT.

In the second step it is mentioned that financial institutions should be transparent and, where possible, obtain consent from its customers. One of the main concerns expressed by the Working Party in its report on this subject was the lack of transparency in the data sharing. The Working Party cited such lack of transparency as a key factor in the violation of fundamental European principles of data protection and in my opinion as would be the case in South Africa when the proposed POPIA is implemented. In light of this they recommend that financial institutions should consider implementing policies that outline the process for transferring personal data to government entities in response to valid and legally binding requests and they further suggest that financial institutions should

[76] Jacqueline Klosek & Lauren Troxclair, Banks Need A Disclosure "Action Plan", Bank Technology News, June 2006, Vol 20, Nr 6.

communicate such policies to customers. In addition to disclosing the potential for personal data transfers, financial institutions should also obtain prior consent from customers for potential personal data transfers, provided such transfers are made pursuant to valid and legally binding requests.

In the third and final step, it is suggested that financial institutions should be broad with consumers and demand specificity from the government and business partner. When making disclosures to consumers and obtaining consumer consent to prospective disclosures, it is advisable to be as broad as possible. On the other hand, when contracting with other parties, it is recommended to include clauses that will restrict such parties from sharing information at all.

Although the above three step procedure is not necessarily intended for a South African audience, I do feel that it could play a significant role in preventing South African banks from subjecting themselves to a similar situation, should the proposed POPIA be enacted. It is therefore suggested that in their contracts or binding schemes with such institutions as SWIFT, cognisance of the above steps should be taken.

4 Basel II and the proposed POPIA

In this chapter I will try to demonstrate how current banking practices and the implementation of Basel II might send off on a collision course with the POPIA. It must however be emphasized that most of the provisions laid down for its implementation is still in its infancy and it is also not currently possible to get access to any of the recommendations made by the various banks related to Basel II, since none of it is publicly available.

4.1 Basel II

To illustrate the functions of Basel II and its relativity to the South African banking industry I find it best to refer to the summary as is noted in the Memorandum on the Objects of the Banks Amendment Bill, 2007:[77]

> *"On 26 June 2004 the International Basel Committee on Banking Supervision published an amended capital framework for banks entitled "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", generally referred to and known as "Basel II". The primary objective of Basel II is to replace the 1988 Capital Accord to further strengthen the soundness and stability of the international banking system by the adoption of stronger risk management practices by the banking industry. Basel II has important implications for the capital frameworks of banks and the regulatory framework and supervisory processes applicable to banks.*
>
> *Given the potential negative effects of not implementing Basel II on the South African banking industry, it is prudent to implement Basel II in its entirety and to amend the legal framework to facilitate its implementation.*

[77] View http://www.treasury.gov.za/legislation/bills/2007/Memoranda%20on%20Objects%20-%20Draft%20Banks%20Amendment%20Bill%202007.pdf (25 August 2007)

An Accord Implementation Forum ("AIF") was established to manage and co-ordinate the implementation of Basel II. The Registrar of Banks chairs the Steering Committee of the AIF and its members include delegates from National Treasury, various departments of the South African Reserve Bank, the banks and the auditing profession. The Regulatory Framework Sub-Committee ("RFSC") of the Steering Committee was tasked to review the current legal framework relating to banks and to identify necessary amendments to give effect to Basel II.

The RFSC identified a number of amendments to the Banks Act that are necessary to give effect to Basel II and assisted the Office of the Registrar of Banks in the drafting of the draft Banks Amendment Bill. The Bill is thus the result of an inclusive and consultative process between this Office, the banking industry and other role-players since 2004.

The proposed implementation date for Basel II is 1 January 2008."

Basel II requires banks to collect and exchange huge amounts of data, including customer data which usually falls under data protection legislation. What is rather surprising is that none of these provisions were specifically made mention of in the Bank Amendments Bill. It is assumed that this data is needed to do the requested ratings in the future. In Europe a draft of the new EU capital requirement framework (EU Council Doc Nr. 12890/05 – "New Directive")[78] was issued. The rating provisions request the collection of huge amounts of data on their bank customers and banks already collect customer data of various kinds, including for example soft facts (like private/family issues of company managers). In a recent fact finding questionnaire by Rainer Knyrim on behalf of the International Chamber of Commerce (ICC)[79], it was found that banks question whether they really have the right to collect and process this data which comes from many different sources and is collected partly without the customers' knowledge. They also contended that the draft of the new directive does not give any useful help in solving this question. A question would be whether the South African drafters have themselves followed through in trying to resolve similar issues.

[78] View http://europa.eu.int/comm/internal_market/bank/regcapital/index_en.htm#capitalrequire (25 August 2007)

[79] View http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Basel_II_questionnaire_and_answers_09_10_2006.pdf (25 August 2007)

The ICC also established that to do ratings and settle credit limits on large customers in Europe who are clients in different banks of a banking group, data needs to be exchanged both EU-wide as well as globally which leads to the well-known data transfer problems. This problem from a South African perspective was discussed under my chapter 3.

It was further implied that experience has shown that the argument of a prevailing interest of the bank is more difficult to argue in discussions with data protection authorities than was thought and international and national laws were not precise enough to serve as a legal basis for a transfer.

In South Africa, this legal basis as referred to above, would for instance be derived from Section 9 (1) (c) of the proposed POPIA where it is stated that personal information may only be processed where the processing is necessary in order to comply with a legal obligation to which the responsible party is subject.

Hence the fact that no reference in the Bank Amendment's Bill is made to data collection and subsequent processes which, in my opinion, would make it difficult for banks to argue that they do in fact have a legal basis for the transfer of data within the ambit of Basel II. In other words, it would be difficult to derive from the said Bill any obligation to collect, process or transfer any personal information. However, without having all the necessary resources available to me, it might be a premature and prejudice statement and I stand to be proven incorrect. It does however raise a viable question and from the experience drawn in Europe, illustrated above, needs to be taken note of.

4.2 Relevant questions

In verifying some of the issues, I will discuss a number of the questions that were asked in the mentioned ICC questionnaire at the hand of answers supplied by an anonymous South African bank.

These questions are as follow:

Question 1:

Does your bank already collect rating data on its customers to fulfil Basel II requirements? Is your bank already collecting or will it collect “soft facts” on its customers? Will it collect sensitive data like race, religion, health or criminal information of key personnel of your customer? Will your bank use data on its customers received from third parties?

The SA bank replied as follow: (My comments in brackets)

South African banks already collect data on most of their customers, however internal rating coverage is not yet complete. The banks retail portfolios are substantially complete and the corporate counterparties anticipate completion by the end of 2007.
Banks collect data on most of their customers; however historic credit vetting data on unrated clients’ is generally in hard copy on file, not electronic. The banks expect to have uniform approach to managing electronic rating data and collect all counterparties’ data in electronic format by the end of 2007 to satisfy Basel II requirements.
Banks collect data on key personnel (e.g. Directors/shareholders) where surety has been provided by them for the counterparty. As far as it would improve the estimation of credit risk, processes to expand data collection would be considered.
Any sensitive data collected is subject to the Constitution of South Africa and where sensitive data is collected it is permitted under specific legislation such as Employment Equity Act etc. (This would qualify under the section 26 exemption to the prohibition on processing of personal information concerning a person’s race in the POPIA).[80]

[80] 26. The prohibition on processing personal information concerning a person's race, as referred to in section 24, does not apply where the processing is carried out -
(a) with a view to identifying data subjects and only where this is essential for that purpose;
(b) for the purpose of assigning a preferential status to a person from a particular ethnic or cultural group with a view to eradicating or reducing actual historical or socio-economic inequalities, provided that the data subject has not indicated any objection thereto in writing.

Bank staff that are dismissed due to criminal offences are listed on The Banking Association REDS data base for use by Human Resources managers within the Banking Industry only. (This would qualify as I assume under the section 30 exemption to the prohibition on processing of personal information concerning a person's criminal behaviour in the POPIA.)[81]

At present entities within a banking group can share counterparty data whilst external data source (Bureau Agencies e.g. Experian & ITC) can be purchased or acquired to enhance risk estimation. Intended Privacy Legislation will require the consent of the customer. (With regards to the further processing principle in section 14 of the POPIA, I doubt whether entities within a banking group would be allowed to share counterpart data unless the preconditions are met.)[82]

---

[81] 30.(1) The prohibition on processing personal information concerning a person's criminal behaviour, as referred to in section 24, does not apply where the processing is carried out by bodies, charged by law with applying criminal law and by responsible parties who have obtained this information in accordance with the law.
(2) The prohibition does not apply to responsible parties who process this information for their own purposes with a view to:
(a) assessing an application by data subjects in order to take a decision about them or
provide a service to them, or
(b) protecting their interests, provided that this concerns criminal offences which have been or, as indicated by certain facts and circumstances, can be expected to be committed against them or against persons in their service.
(3) The processing of this information concerning personnel in the service of the responsible
party must take place in accordance with the rules established in compliance with labour legislation.
(4) The prohibition on processing other personal information, as referred to in section 24, does not apply where this is necessary to supplement the processing of information on criminal behaviour, for the purposes for which this information is being processed.
(5) The provisions of subsections (2) to (4) are likewise applicable to personal information relating to a ban imposed by a court concerning unlawful or objectionable conduct.

[82] 14. (1) Personal information must not be further processed in a way incompatible with a purpose for which it has been collected in terms of principle 2.
(2) For the purposes of assessing whether processing is incompatible, as referred to under subsection (1), the responsible party must take account of the following -
(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been obtained;
(b) the nature of the information concerned;
(c) the consequences of the intended further processing for the data subject;
(d) the manner in which the information has been obtained, and
(e) any contractual rights and obligations existing between the parties.
(3) The further processing of personal information must not be regarded as incompatible as referred to under subsection (1) where -
(a) the processing of the information for that other purpose is authorised by the data subject; or
(b) the source of the information is a publicly available publication; or
(c) non-compliance is necessary -
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal (being
proceedings that have been commenced or are reasonably in contemplation); or
(v) in the interests of national security; or
(d) the processing of the information for that other purpose is necessary to prevent or mitigate a serious and imminent threat to:
(i) public health or public safety; or
(ii) the life or health of the data subject or another individual; or

Question 2:

To settle credit limits on large customers which are clients in different banks of a banking group, will your bank exchange customer/rating data within its banking group or with other banks/third parties? Will this transfer involve cross border data flow outside the EU?

The SA bank replied as follow: (My comments in brackets)

Within a banking group, individual banks will exchange rating data; however sharing with other banks/third parties would be subject to the arrangement between the parties. (In terms of section 9 of the POPIA, I doubt whether this will be allowed unless the exceptions are applied.)[83]
A bank may enquire with another bank for a rating of the client using an industry coding system that qualifies a client's transaction behaviour related to risk profile. E.g.: a cheque issued in settlement of a debt could be verified by the issuing bank i.e. good for funds. (Note my previous comment.)
In South Africa no restriction exists on cross border data flow and South Africa banks will share data with their African and EU operations. (This will change in terms of section 94 of the POPIA.)[84]

The number of questions is numerous and I will not go through all of them. The point that I do however try to establish is that there is definitely areas of conflict between the implementation of Basel II and the proposed POPIA. These are not necessarily problems that are insurmountable. There are enough exclusions in the proposed POPIA that might render the processing under Basel II legitimate, but from a practical banking perspective it might prove costly.

(e) the information is used for historical, statistical or scientific purposes where the responsible party has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes and will not be published in a
form from which the identity of the data subject may be established or inferred; or
(f) the further processing of the information is in accordance with an authority granted
under section 33 (exemptions) of this Act.

[83] Ibid note 82.

[84] Refer to pages 13 and 14.

I do not believe that proposed POPIA sufficiently or clearly covers the Basel II data protection issues, and in the face of such uncertainty, banks will have to adopt a conservative approach and try and obtain customer consent in most cases, at a significant procedural and monetary cost to the banks.

5 Conclusion

A survey of access to information laws and practices in 14 countries was done by the Open Society Initiative and published in its Justice in Action Series, tilted, Transparency and Silence. They had the following to say about South Africa:

> *"South Africa, the only monitored country in Africa with a freedom of information law in place, demonstrated greater compliance with the right to information than the other four African countries. However, only 19 percent of the requests submitted in South Africa yielded a compliant outcome and only 13 percent yielded information. This is by far the lowest score of the seven monitored countries with freedom of information laws. Justice Initiative monitoring exercises in both 2003 and 2004 highlighted serious problems with the implementation of South Africa's Promotion to Access of Information Act (Act No. 2 of 2 February 2000), and these problems resulted in high levels of mute refusals in response to requests. Although the law is strong on paper, it has proved complex to implement in practise, and there have not been sufficient efforts to make its implementation a priority. Better implementation might yet make it a model for the region."*

Clearly this is the last sort of comment that South Africa needs on the implementation of its proposed POPIA. Currently, as the draft stands, it is however not unforeseeable that such comment might well be read into its implementation, since some of its provisions might also prove too complex to implement in practise, especially seen from the banking industry's perspective.

Some of the issues that were raised in this thesis are for instance the cross border data transfer problems related to payment orders. Other problems indicated were those concerning fraud, Basel II and the legally non-binding codes of conduct that is currently laying the guidelines for banking practices with regards to its consumers.

The question would be whether there is a golden one rule solution. I sincerely doubt this. It is my contention that an array of various factors must play a role in seeing the proposed POPIA through to its successful implementation. Such factors would include safe harbour agreements, technological solutions, and sector specific regulations in the form of privacy code of conducts.

For South African banks to operate successfully in Africa, specifically in the SADC region (SADC stands for 'Southern African Development and Economic Community' and refers to 14 African nations[85] in Southern Africa, who have signed a mutual trade and co-operation agreement) it is my suggestion that South Africa sign a safe harbour agreement[86] with the other members of SADEC, similar to that as between the USA and the EU, but with the exception that it also makes provision for financial institutions,. None of theses countries[87] currently make provision for data protection in its laws. Without such an agreement, banks might be strained along in subjecting themselves to unnecessarily high costs in its strive to comply with the proposed POPIA. In signing such an agreement however, time limits must be set on these countries to implement similar legislation, encouraging them to step up its own democratic values in ensuring sufficient privacy measures and achieving the objectives and vision as set by SADC.[88] This would then set a standard for the rest of Africa and hopefully spirit them on to reach similar goals.

It is also suggested that similar safe harbour agreements must be concluded between South Africa and some of its other trading partners. Some of these major trading partners include the United Kingdom, the United States, Germany, Italy,

---

[85] These countries include Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Kingdom of Swaziland, Tanzania, Zambia and Zimbabwe. For further information, see http://www.sadc.int/home.php (24 August 2007)

[86] See http://www.export.gov/safeharbor/ (24 August 2007) for a detailed discussion on the safe harbour agreement.

[87] Ibid note 85.

[88] The objectives of SADC as stated in Article 5 of the Treaty are to: Achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through regional integration; Evolve common political values, systems and institutions; Promote and defend peace and security; Promote self-sustaining development on the basis of collective self-reliance, and the interdependence of Member States; Achieve complementarity between national and regional strategies and programmes; Promote and maximise productive employment and utilisation of resources of the Region; Achieve sustainable utilisation of natural resources and effective protection of the environment; Strengthen and consolidate the long-standing historical, social and cultural affinities and links among the people of the Region.

Belgium, and Japan, although it would only be foreseen that such an agreement be reached between South Africa and the United States, since the other five do make provision for adequate measures.

Technological advances also have a role to play. Paul Rosenzweig and Alane Kochems[89] explain that technology is both a problem and a solution for the issues posed by enhanced information collection systems. It can facilitate access to and the accumulation of large amounts of data; however, if that access is not properly managed, the information can be misused. When designed with proper procedures and protections and combined with oversight, technology can provide a reasonable balance between security and privacy. They continue by stating that in properly determining how best to enhance both liberty and security, it is useful to have some basic principles for assessing data protection technologies. They contend that such a list might include the following:

- The data protection technology should allow for clear audit tracks to prevent data alteration or identify when data have been changed.
- The technology should have a means to provide graduated levels of access to the data.
- The technology should have protocols for enforcing the confidentiality and security of the data.

There are multiple approaches to securing data. One means is following one of the many published information security standards; another is to protect the most sensitive data through encryption. They conclude by stating that controlling access to data and making sure that entities only have the appropriate level of access is critical if privacy interests are to be protected. Various software companies have adapted its data collection programs to make provision for legislation. A number of academic writers[90] are also of the point of view that the solution would be in the

[89] Their article titled "Data Protection: Safeguarding Privacy in a New Age of Technology" can be viewed at: http://www.heritage.org/Research/HomelandSecurity/lm16.cfm (26 August 2007)

[90] Lessig, Lawrence in "Code and other Laws of Cyberspace", Reidenberg, Joel R. in "Lex Informatica: The Formulation of Information Policy Rules Through Technology", Texas Law Review, University of Texas at Austin School of Law Publications, 76 (3) 1998 pp. 553-584, Rotenberg, Marc in "Fair Information Practices and the Architecture of Privacy" (What Larry Doesn't Get), Stanford Technology Law Review, Cite as: 2001 Stan. Tech. L. Rev. 1 http://stlr.stanford.edu/STLR/Articles/01_STLR_1 (22 August 2007)

code and that lex informatica could be a useful policy device. But this is a discussion in its own right. The fact that technology would and in fact must play a role is unmistakable and its contributory role in the banking industry could provide solutions to successful implementation of the proposed POPIA.

The last and probably most crucial factor is the facilitation of sector based codes of conduct. The solution does not necessarily arrive with the issuing of the codes themselves, but rather through a pre-emptive strike and pro-active based effort on behalf of the specific sectors, in this case the banking industry, to submit such codes to the Commissioner. If the banks sit back and wait for the Commissioner to issue these codes, problems might arise as to the interim position on the implementation and interpretation of the proposed POPIA. Having regard to the specific related problems that might arise from the banking industry's perspective, as was mentioned earlier, courts could create precedents[91], which in the absence of such co-regulatory structures, could be detrimental to the industry as a whole. With its sector based knowledge, it is therefore suggested that the banking industry, or financial industry as a whole, make sure that they have these codes of conduct or privacy codes ready for submission when the proposed POPIA becomes enacted, thereby annihilating any room for an uncertain interim period that might be subject to scrutiny.

[91] See for instance Unitas v Van Wyk & Naude case nr 231/2005. Sec 50 – meaning of "required" for exercise or protection of right – when available to compel pre-action production. The threshold of "required" was set very high due to uncertainty on whether to use the Promotion to Access of Information Act (PAIA). PAIA was not the appropriate remedy. Discovery would probably have been successful in this delictual action.

6 Bibliography

6.1 Books and Articles

Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at http://web.uvic.ca/polisci/bennett/ accessed on 05 August 2007.

Berkvens Prof., Jan, M.A. and Schauss, Marc N; "The Amended proposal for an EC Directive on Data Protection; Progress on the face of it, disillusion after scrutiny"; Butterworth's Journal of International Banking and Financial Law, 1993, February.

Botha, Christo; Statutory Interpretation: An introduction for students; 4th edition; Juta; 2005.

Bygrave L.A.; "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling"; Computer Law and Security Report; 2001; Vol 17 pages 17-24 available at http://folk.uio.no/lee/publications/ accessed on 03 August 2007.

Bygrave L.A.; Data protection: Approaching Its Rationale, Logic and Limits; Kluwer Law International; The Hague 2002.

Currie, Iain; "The Data Provisions of the National Credit Act" available at http://wwwserver.law.wits.ac.za/mi/privacy/nationalcreditact.htm accessed on 05 August 2007.

Fisher-French, Maya; "Fica'd to death"; Mail and Guardian Online; 31 July 2006; available at http://www.mg.co.za/personalfinance/articlePage.aspx?articleid=279307&area=/personal_finance/pers_fin_banking/ accessed on 07 August 2007.

Knyrim, Rainer; "ICC-Fact Finding Questionnaire Basel II and Data Protection Questionnaire and Answers"; Department of Policy and Business Practices; International Chamber of Commerce; 9 October 2006; available at http://www.iccwbo.org/uploadedFiles/ICC/policy/e-

business/pages/Basel_II_questionnaire_and_answers_09_10_2006.pdf accessed on 26 August 2007.

Lessig, Lawrence; "Code and other Laws of Cyberspace"; Basic Books; 1999; pages 142-163.

Neethling J, Potgieter JM and Visser PJ; Neethling's Law of Personality; Butterworths; Durban; 2005.

Reidenberg, Joel R.; "Lex Informatica: The Formulation of Information Policy Rules Through Technology"; Texas Law Review; University of Texas at Austin School of Law Publications; 76 (3) 1998; pp. 553-584.

Roos, A; "The Law of Data (Privacy) Protection: A Comparative and Theoretical Study"; LLD thesis; UNISA; October 2003.

Rosenzweig Paul and Kochems Alane; "Data Protection: Safeguarding Privacy in a New Age of Technology"; The heritage Foundation; March 23; 2005 available at http://www.heritage.org/Research/HomelandSecurity/lm16.cfm accessed on 26 August 2007.

Rotenberg, Marc; "Fair Information Practices and the Architecture of Privacy" (What Larry Doesn't Get); Stanford Technology Law Review; 2001 Stan. Tech. L. Rev. 1 available at http://stlr.stanford.edu/STLR/Articles/01_STLR_1 accessed on 22 August 2007.

6.2 List of Judgements/Decisions

SOUTH AFRICA

Bernstein ao v Bester ao NNO 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC).

Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao 1993 (2) SA 451 (A).

Jansen Van Vuuren ao NNO v Kruger 1993 (4) SA 842 (A).

Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao 1994 (3) SA 56 (W);1995 (4) SA 293 (A).

Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao 1991 (2) SA 117 (W).

6.3 Legislation / Statutes

SOUTH AFRICA

Banks Amendment Bill, 2007

Constitution of the Republic of South Africa,1996.

Electronic Communications and Transactions Act 25 of 2002.

Financial Advisory and Intermediary Services Act 37 of 2002.

National Credit Act 34 of 2005.

Promotion of Access to Information Act 2 of 2000.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

SA Reserve Bank Act 90 of 1989.

AUSTRALIA

Privacy Act, 1988.

Privacy Amendment (Private Sector) Act, 2000.

CANADA

Personal Information Protection and Electronic Documents Act, 2000.

GERMANY

Germany's Federal Data Protection Act.

UNITED KINGDOM

Data Protection Act, 1998.

NETHERLANDS

Personal Data Protection Act 2000 (Wet Bescherming Persoonsgegevens)

NEW ZEALAND

Privacy Act, 1993.

6.4 Conventions, Directives, Guidelines and Declarations

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950.

Council of Europe Electronic Communications Privacy Directive June 25, 2002.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (EU Directive).

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (ISDN Directive).

Organisation for Economic Co-operation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981.

Organisation for Economic Co-operation and Development (OECD) "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

South African Law Reform Commission Discussion papers available at http://www.doj.gov.za/salrc/dpapers.htm accessed on 04 August 2007.

Working Document (WP74); Transfers of personal data to third countries: "Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers"; 11639/02/EN WP 74 available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf. accessed on 10 August 2007.